

I. Amendments to the Claims

Please amend the claims as follows with the following version of the claims in accordance with revised 37 CFR § 1.121.

1. (Currently Amended) A method for controlling access to protected resources within a distributed data processing system, the method comprising:

receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

determining that the single-use token is a domain token;

generating a client authorization credential request;

sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated within a common domain;

generating a response to the request;

refreshing the single-use token; and

sending the response and the refreshed single-use token to the client.

2. (Currently Amended) The method of claim 1 further comprising:

receiving ~~determining that the single-use token is a~~ single-use service token, wherein the single-use a service token is issued by the first server; and

refreshing the single-use service token at the first server.

3. (Original) The method of claim 1 wherein the session information in the single-use token is a session key.

4. (Canceled).

5. (Currently Amended) The method of claim 1 4 further comprising:

validating at the second server the single-use domain token associated with the client or the user of the client and the
5 single-use domain token associated with the first server;

generating the client authorization credential;

refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and

10 sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

15 6. (Original) The method of claim 5 further comprising:

storing the client authorization credential at the first server;

generating a single-use service token associated with the client or the user of the client;

20 and sending to the client the single-use service token along with the response and the single-use domain token.

7. (Original) The method of claim 1 further comprising:

25 receiving a login request from the client at the second server;

challenging the client to provide authentication data;
receiving authentication data from the client;

authenticating the client; generating a single-use domain token associated with the client or the user of the client;

30 generating an authentication response; and
sending the authentication response and the single-use domain token to the client.

8. (Original) The method of claim 7 further comprising:
determining that the login request is a redirected request
from the first server; and
modifying the authentication response to redirect the
5 client to the first server.

9. (Currently Amended) An apparatus for controlling access to
protected resources within a distributed data processing system,
the apparatus comprising:

10 means for receiving at a first server from a client a
request to access a protected resource and a single-use token
associated with the client or a user of the client;

means for validating the single-use token, wherein the
single-use token comprises session information for performing
15 session management with respect to the client;

means for determining that the single-use token is a domain
token;

means for generating a client authorization credential
request;

20 means for sending to a second server the client
authorization credential request, the single-use domain token
associated with the client or the user of the client, and a
single-use domain token associated with the first server,
wherein the first server and the second server are operated
25 within a common domain;

means for generating a response to the request;

means for refreshing the single-use token; and

means for sending the response and the refreshed single-use
token to the client.

30 10. (Currently Amended) The apparatus of claim 9 further
comprising:

means for ~~receiving~~ ~~determining that the single-use token~~
is a single-use service token, wherein the single-use a service
token is issued by the first server; and

means for refreshing the single-use service token at the
first server.

11. (Original) The apparatus of claim 9 wherein the session
information in the single-use token is a session key.

12. (Canceled).

13. (Currently Amended) The apparatus of claim 9 ~~12~~ further
comprising:

means for validating at the second server the single-use
domain token associated with the client or the user of the
client and the single-use domain token associated with the first
server;

means for generating the client authorization credential;

means for refreshing at the second server the single-use
domain token associated with the client or the user of the
client and the single-use domain token associated with the first
server; and

means for sending to the first server the client
authorization credential, the refreshed single-use domain token
associated with the client or the user of the client, and the
refreshed single-use domain token associated with the first
server.

14. (Original) The apparatus of claim 13 further comprising:

means for storing the client authorization credential at
the first server;

means for generating a single-use service token associated with the client or the user of the client; and

means for sending to the client the single-use service token along with the response and the single-use domain token.

5

15. (Original) The apparatus of claim 9 further comprising:

means for receiving a login request from the client at the second server;

means for challenging the client to provide authentication data;

10

means for receiving authentication data from the client;

means for authenticating the client;

means for generating a single-use domain token associated with the client or the user of the client;

15 means for generating an authentication response; and

means for sending the authentication response and the single-use domain token to the client.

16. (Original) The apparatus of claim 15 further comprising:

20 means for determining that the login request is a redirected request from the first server; and

means for modifying the authentication response to redirect the client to the first server.

25

17. (Currently Amended) A computer program product on a computer readable medium for controlling access to protected resources within a distributed data processing system, the computer program product comprising:

5 instructions for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

instructions for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

10 instructions for determining that the single-use token is a domain token;

instructions for generating a client authorization credential request;

15 instructions for sending to a second server the client authorization credential request, the single-use domain token associated with the client or the user of the client, and a single-use domain token associated with the first server, wherein the first server and the second server are operated
20 within a common domain;

instructions for generating a response to the request;

instructions for refreshing the single-use token; and

instructions for sending the response and the refreshed single-use token to the client.

25 18. (Currently Amended) The computer program product of claim 17 further comprising:

instructions for receiving determining that the single-use
token is a single-use service token, wherein the single-use a-
30 service token is issued by the first server; and

instructions for refreshing the single-use service token at the first server.

19. (Original) The computer program product of claim 17 wherein the session information in the single-use token is a session key.

5 20. (Canceled).

21. (Currently Amended) The computer program product of claim 17 ~~20~~ further comprising:

10 instructions for validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;

instructions for generating the client authorization credential;

15 instructions for refreshing at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server; and

20 instructions for sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

25 22. (Original) The computer program product of claim 21 further comprising:

30 instructions for storing the client authorization credential at the first server; instructions for generating a single-use service token associated with the client or the user of the client; and

instructions for sending to the client the single-use service token along with the response and the single-use domain token.

5 23. (Original) The computer program product of claim 17 further comprising:

instructions for receiving a login request from the client at the second server;

10 instructions for challenging the client to provide authentication data;

instructions for receiving authentication data from the client; instructions for authenticating the client;

instructions for generating a single-use domain token associated with the client or the user of the client;

15 instructions for generating an authentication response; and

instructions for sending the authentication response and the single-use domain token to the client.

20 24. (Original) The computer program product of claim 23 further comprising:

instructions for determining that the login request is a redirected request from the first server; and

instructions for modifying the authentication response to redirect the client to the first server.